CLAIMS:

What is claimed is:

1. A method in a data processing system for protecting data from damage, the method comprising:

journaling the data to form journaled data;

determining whether a virus is present in the data processing system after journaling of data has begun; and

responsive to an identification of the virus, restoring the data using the journaled data.

2. The method of claim 1 further comprising:

responsive to an absence of an identification of the virus, discarding the journaled data.

3. The method of claim 1, wherein the determining step comprises:

performing pattern matching.

4. The method of claim 3, wherein the performing step includes:

comparing a set of actions occurring within the data processing system with a set of patterns.

5. The method of claim 1, wherein the data is located in a storage device external to the data processing system.

6. The method of claim 1 further comprising:

recording a sequence of actions occurring within the data processing system.

7. The method claim 1, wherein the data is data accessed by a process within the data processing system.

8. The method of claim 1 further comprising:

responsive to an identification of the virus, blocking access to the data by a process accessing the data.

9. The method of claim 1 further comprising:

responsive to an identification of the virus, generating an indication halting a process accessing the data.

10. The method of claim 1, wherein the data journaled is data accessed by a single process and maintained until a determination is made that the single process is eliminated as a virus candidate.

11. The method of claim 1, wherein the journaled data is stored in a protected memory accessible only by the method.

12. The method of claim 11, wherein the journaled data is stored in a data structure located in a protected memory inaccessible by a process.

13. A method in a data processing system for repairing damage to data, the method comprising:

saving a state of a data object in response to a request to access the data object by a process;

performing pattern matching of a set of actions taken within the data processing system; and

determining whether an unauthorized intrusion has occurred in response to performing pattern matching.

14. The method of claim 13, wherein the performing step comprises:

comparing the set of actions to a pattern from a set of patterns to form a comparison;

determining whether the comparison indicates that the unauthorized intrusion has occurred; and

responsive to an absence of the unauthorized intrusion, repeating the comparing step using another pattern from the set of patterns.

15. The method of claim 13, wherein the performing step comprises:

matching patterns with the set of actions;

determining whether the unauthorized intrusion has occurred;

if an intrusion is absent, determining whether a time threshold has been reached; and

if an absence of a reaching of the time threshold is present, repeating the matching step using another set of actions.

16. The method of claim 14, wherein match between the pattern and the set of actions identifies an absence of the unauthorized intrusion.

17. The method of claim 14, wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion.

18. The method of claim 13, wherein the intrusion is caused by a virus.

19. The method of claim 13, wherein the intrusion is caused by an authorized user input.

20. The method of claim 13 further comprising:

saving a state of all data objects within the data processing system.

21. The method of claim 13, wherein the data object is located in a storage device external to the data processing system.

22. An intrusion protection system for use in a data processing system comprising:

a sensor filter, wherein the sensor filter receives requests to access data within the data processing system from a process;

a pattern matcher, wherein the pattern matcher receives actions initiated by the process, compares the actions to a pattern to form a comparison, determines whether an unauthorized intrusion has occurred, generates a first indication in response to an identification of an absence of an unauthorized intrusion, and generates a second indication to restore the data to a prior state in response to an identification of the unauthorized intrusion; and

a journaler, wherein the journaler journals data in response to accessing of the data and restores the data to the prior state in response to the indication by the pattern matcher, wherein the data is journaled until the first indication is generated by the pattern matcher.

23. The intrusion protection system of claim 22, wherein the intrusion protection system is located within an operating system.

24. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes as set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to journal the data to form journaled data; determines whether a virus is present in the data processing system after journaling of data has begun; and restores the data using the journaled data in response to an identification of the virus.

25. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to save a state of a data object in response to a request to access the data object by a process; perform pattern matching of a set of actions taken within the data processing system; and determine whether an unauthorized intrusion has occurred in response to performing pattern matching.

26. A data processing system for protecting data from damage, the data processing system comprising:

journaling means for journaling the data to form journaled data;

determining means for determining whether a virus is present in the data processing system after journaling of data has begun; and

restoring means, responsive to an identification of the virus, for restoring the data using the journaled data.

27. The data processing system of claim 26 further comprising:

discarding means, responsive to an absence of an identification of the virus, for discarding the journaled data.

28. The data processing system of claim 26, wherein the determining means comprises:

means for performing pattern matching.

29. The data processing system of claim 28, wherein the performing means includes:

means for comparing a set of actions occurring within the data processing system with a set of patterns.

30. The data processing system of claim 26, wherein the data is located in a storage device external to the data processing system.

31. The data processing system of claim 26 further comprising:

recording means for recording a sequence of actions occurring within the data processing system.

32. The data processing system claim 26, wherein the data is data accessed by a process within the data processing system.

33. The data processing system of claim 26 further comprising:

blocking means, responsive to an identification of the virus, for blocking access to the data by a process accessing the data.

34. The data processing system of claim 26 further comprising:

generating means, responsive to an identification of the virus, for generating an indication halting a process accessing the data.

35. The data processing system of claim 26, wherein the data journaled is data accessed by a single process and maintained until a determination is made that the single process is eliminated as a virus candidate.

36. The data processing system of claim 26, wherein the journaled data is stored in a protected memory accessible only by the method.

37. The data processing system of claim 36, wherein the journaled data is stored in a data structure located in a protected memory inaccessible by the process.

38. A data processing system for repairing damage to data, the data processing system comprising:

saving means for saving a state of a data object in response to a request to access the data object by a process;

performing means for performing pattern matching of a set of actions taken within the data processing system; and

determining means for determining whether an unauthorized intrusion has occurred in response to performing pattern matching.

39. The data processing system of claim 38, wherein the performing means comprises:

means for comparing the set of actions to a pattern from a set of patterns to form a comparison;

means for determining whether the comparison indicates that the unauthorized intrusion has occurred; and

means, responsive to an absence of the unauthorized intrusion, for repeating the comparing step using another pattern from the set of patterns.

40. The data processing system of claim 38, wherein the performing means comprises:

means for matching patterns with the set of actions;

means for determining whether the unauthorized intrusion has occurred;

means, if an intrusion is absent, for determining whether a time threshold has been reached; and

means, if an absence of a reaching of the time threshold is present, for repeating the matching step using another set of actions.

41. The data processing system of claim 39, wherein match between the pattern and the set of actions identifies an absence of the unauthorized intrusion.

42. The data processing system of claim 39, wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion.

43. The data processing system of claim 38, wherein the intrusion is caused by a virus.

44. The data processing system of claim 38, wherein the intrusion is caused by an authorized user input.

45. The data processing system of claim 38 further comprising:

saving means for saving a state of all data objects within the data processing system.

46. The data processing system of claim 38, wherein the data object is located in a storage device external to the data processing system.

47. A computer program product in a computer readable medium for protecting data from damage, the computer program product comprising:

first instructions for journaling the data to form journaled data;

second instructions for determining whether a virus is present in the data processing system after journaling of data has begun; and

third instructions, responsive to an identification of the virus, for restoring the data using the journaled data.

48. The computer program product of claim 47 further comprising:

fourth instructions, responsive to an absence of an identification of the virus, for discarding the journaled data.

49. The computer program product of claim 47, wherein the second instructions comprises:

sub-instructions for performing pattern matching.

50. The computer program product of claim 47, wherein the sub-instructions for performing includes:

instructions for comparing a set of actions occurring within the data processing system with a set of patterns.

51. The computer program product of claim 47, wherein the data is located in a storage device external to the data processing system.

52. The computer program product of claim 47 further comprising:

fourth instructions for recording a sequence of actions occurring within the data processing system.

53. The computer program product claim 47, wherein the data is data accessed by a process within the data processing system.

54. The computer program product of claim 47 further comprising:

fourth instructions, responsive to an identification of the virus, for blocking access to the data by a process accessing the data.

55. The computer program product of claim 47 further comprising:

fourth instructions, responsive to an identification of the virus, for generating an indication halting a process accessing the data.

56. The computer program product of claim 47, wherein the data journaled is data accessed by a single process and maintained until a determination is made that the single process is eliminated as a virus candidate.

57. The computer program product of claim 47, wherein the journaled data is stored in a protected memory accessible only by the method.

58. The computer program product of claim 57, wherein the journaled data is stored in a data structure located in a protected memory inaccessible by the process.

59. A computer program product in a computer readable medium for repairing damage to data, the computer program product comprising:

first instructions for saving a state of a data object in response to a request to access the data object by a process;

second instructions for performing pattern matching of a set of actions taken within the data processing system; and

third instructions for determining whether an unauthorized intrusion has occurred in response to performing pattern matching.

60. The computer program product of claim 59, wherein the second instructions comprises:

first sub-instructions for comparing the set of actions to a pattern from a set of patterns to form a comparison;

second sub-instructions for determining whether the comparison indicates that the unauthorized intrusion has occurred; and

third sub-instructions, responsive to an absence of the unauthorized intrusion, for repeating the comparing step using another pattern from the set of patterns.

61. The computer program product of claim 59, wherein the second instructions comprises:

first sub-instructions for matching patterns with the set of actions;

second sub-instructions for determining whether the unauthorized intrusion has occurred;

third sub-instructions, if an intrusion is absent, for determining whether a time threshold has been reached; and

fourth sub-instructions, if an absence of a reaching of the time threshold is present, for repeating the matching step using another set of actions.

62. The computer program product of claim 60, wherein match between the pattern and the set of actions identifies an absence of the unauthorized intrusion.

63. The computer program product of claim 60, wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion.

64. The computer program product of claim 59, wherein the intrusion is caused by a virus.

65. The computer program product of claim 59, wherein the intrusion is caused by an authorized user input.

66. The computer program product of claim 59 further comprising:

fourth instructions for saving a state of all data objects within the data processing system.

67. The computer program product of claim 59, wherein the data object is located in a storage device external to the data processing system.